CLAIM

[1] A remote-access VPN mediating method in a system wherein: a virtual private network, hereinafter referred to as VPN, client units and a VPN gateway unit are connected to an IP network; communication units are connected to a local area network placed under the management of the VPN gateway unit; and a remote-access VPN by a tunneling protocol is implemented between an arbitrary one of VPN client units and the VPN gateway unit connected to said IP network and an arbitrary one of the communication units connected to the local area network placed under the management of the VPN gateway unit; said method comprising the steps of:

(a) sending an access control list containing information indicative of a private IP address assigned to said communication unit to a mediating apparatus on said IP network from said VPN gateway unit;

(b) storing said access control list by said mediating apparatus in correspondence to said VPN gateway unit;

(c) retrieving an IP private address corresponding to said VPN gateway unit in response to a request from said VPN client unit, acquiring the private IP address of the corresponding communication unit from said access control list, sending the acquired private IP address to said VPN client unit, sending the IP address of said VPN client unit to said VPN gateway unit, generating mutual authentication information for setting up an authenticated encrypted tunnel between said client VPN unit and said gateway unit, and sending said mutual authentication information to both of said VPN client unit and said gateway unit; and

(d) setting up said authenticated encrypted tunnel between said VPN client unit and said gateway unit by use of said mutual authentication information, and implementing remote access through said encrypted tunnel

by use of the private IP address of said communication unit.

[2] The remote-access mediating method of claim 1, wherein said access control list contains attribute information about said VPN client unit.

[3] The remote-access VPN mediating method of claim 2, wherein said step (a) includes a step of encrypting a communication channel between said mediating apparatus and said VPN gateway unit or a VPN gateway management unit having an authority of its management, and sending said access control list from said VPN gateway unit to said mediating apparatus.

[4] The remote-access VPN mediating method of claim 2 or 3, wherein said step (b) includes steps of: authenticating said VPN gateway unit by said mediating apparatus; and storing an access control list for said VPN client unit sent from said VPN gateway unit when the authentication is successful.

[5] The remote-access VPN mediating method of claim 2 or 3, wherein said step (c) includes the steps of:

(c-0) on receiving a request for retrieval of an IP address assigned to said VPN gateway unit from said VPN client unit, verifying whether said VPN client unit has an authority of access to said VPN gateway unit; and only when said VPN client unit has said access authority,

(c-1) referring to an access control list, and acquiring the private IP address assigned to said communication unit;

(c-2) searching a domain name server to acquire the IP address assigned to said VPN gateway unit;

(c-3) encrypting a communication channel between said mediating apparatus and said VPN client unit, and sending the IP address of said VPN gateway unit and the private IP address of said communication unit to said VPN client unit;

(c-4) encrypting a communication channel between said mediating

apparatus and said VPN gateway unit, and sending to said VPN gateway unit a global IP address of said VPN gateway unit and said attribute information about said VPN client unit described in said access control list;

said step (d) including the steps of:

(d-1) generating said mutual authentication information for authentication between said VPN client unit and said VPN gateway unit;

(d-2) encrypting the communication channel between said mediating apparatus and said VPN client unit, and sending to said VPN client unit information necessary for mutual authentication between said mediating apparatus and said VPN gateway unit; and

(d-3) encrypting the communication channel between said mediating apparatus and said VPN gateway unit, and sending to said VPN gateway unit information necessary for mutual authentication between said mediating apparatus and said VPN client unit.

[6] The remote-access VPN mediating method of claim 5, comprising the steps:

wherein, at the time of setting up the encrypted tunnel between said VPN client unit and said VPN gateway unit, said VPN gateway unit performs at least one of: a function of determining the private IP address to be given to said VPN client unit on the basis of said attribute information on said VPN client unit sent from said mediating apparatus, and giving the determined private IP address to said VPN client unit; a function of determining a VLAN to be accommodated on the basis of said attribute information about said VPN client unit, a gateway address, an internal DNS address, a WINS server address, etc.; and a function of changing packet filtering setting of said VPN gateway unit on the basis of said attribute information; and

wherein when the tunnel established between said VPN gateway unit

and said VPN client unit is disconnected or no communication has been conducted via said tunnel for a predetermined period of time, said VPN gateway unit performs tunnel cleanup processing, processing for returning the private IP address assigned to said VPN client unit, and restoring the setting of the packet filtering of said VPN gateway unit used for said VPN client unit concerned.

[7] The remote-access VPN mediating method of claim 2 or 3, wherein: said step (c) includes wherein said VPN client unit captures a DNS query transferred from an in-unit application or another VPN client unit, then collates the source address and contents of said query with filtering conditions, and, if they match the conditions, converts said query to a query to said mediating apparatus; said step (d) includes a step setting/updating the tunneling protocol configuration management information on the basis of an answer to said query; and said step (e) includes a step of initializing the tunnel as required, passing the private IP address of the communication unit specified by said mediating unit, as the result of said DNS query, to the application of the query source.

[8] The remote-access VPN mediating method of claim 5, wherein said step (c) wherein said VPN client unit issues a certificate by an SPKI scheme, and another VPN client unit having received said certificate sends to said mediating apparatus a request for retrieval of the IP address assigned to said VPN gateway unit.

[9] A remote-access VPN mediating apparatus which built on an IP network to implement a remote-access VPN in a system wherein: VPN client units and a VPN gateway unit are connected to the IP network; communication units are connected to a local area network placed under the management of the VPN gateway unit; and a remote-access VPN by a

tunneling protocol is implemented between an arbitrary one of said VPN client units and said VPN gateway unit connected to said IP network and an arbitrary one of said communication units connected to said local area network placed under the management of said VPN gateway unit; said apparatus comprising:

ACL storage means for storing an access control list, hereinafter referred to as ACL, sent from said VPN gateway unit and containing information indicative of the private IP address assigned to said communication unit;

authentication/access authorization control means for authenticating said VPN client unit and said gateway unit, and for executing access authorization control;

IP address acquiring means for referring to said access control list to acquire the private IP address assigned to said communication unit, and for searching a domain name server to acquire the IP address assigned to said VPN gateway unit;

authentication information generating means for generating mutual authentication information for setting up an encrypted tunnel between said VPN client unit and said VPN gateway unit; and

communication means for sending the IP address of said VPN gateway unit, the private IP address of said communication unit and said mutual authentication information to said VPN client unit, and for sending the IP address of said PN client unit and said mutual authentication information to said VPN gateway unit.

[10] The mediating apparatus of claim 9, wherein said communication means includes encryption means for encrypting communications between said mediating apparatus and said VPN client unit, and communications

between said mediating apparatus and said VPN gateway unit.

[11] The mediating apparatus of claim 9, wherein said authentication/access authorization control means: authenticates said VPN client unit; and only when the authentication is successful, causes said IP address acquiring means to query the domain name server about the IP address assigned to said VPN gateway unit and acquire said IP address; causes said mutual authentication information generating means to generate said mutual authentication information; and causes said communication means to send the acquired IP address, the private IP address assigned to said communication means, and said generated mutual authentication information to said VPN client unit.

[12] The mediating apparatus of claim 9, wherein said authentication/access authorization control means: decides whether said VPN client unit has the authority to retrieve the IP address assigned to said VPN gateway unit; and only when the VPN gateway unit has said authority, causes said IP address acquiring means to query the domain name server about the IP address assigned to said VPN gateway unit and acquire said IP address; causes said mutual authentication information generating means to generate said mutual authentication information; and causes said communication means to send the acquired IP address, the private IP address assigned to said communication unit, and said generated mutual authentication information to said VPN client unit.

[13] The mediating apparatus of claim 11 or 12, wherein said authentication/access authority control means: authenticates said VPN gateway unit; and only when the authentication is successful, causes said communication means to send the IP address assigned to said VPN client unit and said mutual authentication information to said VPN gateway unit.

[14] The mediating apparatus of any one of claims 9 to 13, wherein said

authentication/access authorization control means authenticates said VPN client unit and said VPN gateway unit by an SPKI (Simple Public Key Infrastructure) scheme, and/or executes access authorization control.

[15] The mediating apparatus of any one of claims 9 to 13, wherein said authentication/access authorization control means authenticates said VPN client unit and said VPN gateway unit by a PKI (Public Key Infrastructure) scheme.